Effective Date: 6/1/17

Data Classification Standard

Purpose

The Data Classification Standard is intended to provide standardization for identification, classification, and labeling of information assets, to facilitate the use of appropriate security, privacy, and compliance measures to protect the confidentiality, integrity, and availability of data/information and associated Information Technology (IT) Security Policy objectives.

Standard

All information assets managed by DOA/DET must be identified, categorized, and labeled, as Classified, Restricted, Sensitive, or Public.

These labels are determined by the impact level of high, moderate, low, or none as determined by the scores of three principles of security: 1) confidentiality, 2) integrity, and 3) availability. Classified information assets have a high impact level, restricted information assets have a moderate impact level, sensitive and public information assets have a low impact levels. See Appendix A for instructions to determine appropriate classification/label.

Examples of each classification label include

Classified information assets include items:

- identified with a High impact level
- identified by an Agency as confidential
- subject to regulatory or compliance requirements (e.g., FTI, HIPAA, IRS, DMCA, PCI, PHI, PII, etc.)
- that contain personally identifiable information (PII), personal health information (PHI/ePHI) or state/federal tax information
- with contractual language requiring a confidential or high classification level for information/data (proprietary data) (e.g., CMS/CARES)
- NOTE: Information assets at this level must limit access to authorized individuals only and must employ encryption of data at rest, in use and in transit (AC-21).

Restricted information assets include items:

- identified with a Moderate impact level
- identified by an Agency as restricted (e.g. internal process/procedure documentation, security event logs, system configuration information)

Effective Date: 6/1/17

- NOTE: Information assets at this level must limit access to authorized individuals only and may employ encryption of data at rest, in use and in transit (AC-21).

Sensitive information assets include items:

- identified with a Low impact level
- identified by an Agency as sensitive (e.g. internal policies)
- NOTE: Information assets at this level may be shared with individuals external to DOA and do not require encryption of data at rest, in use, or in transit (AC-21).

Public information assets include items:

- identified with no impact level
- identified by an Agency as public
- information can be shared publicly
- NOTE: Information assets at this level may be shared publicly and does not require encryption of data at rest, in use, or in transit (AC-21). Publicly accessible information for DOA must be approved by the Public Information Officer for content control (AC-22).

Information assets that have data at multiple classifications must be identified, categorized, and labeled as the highest identified classification level.

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.
- Information Asset – All DET/State information and DET/State information systems and environments.

Compliance References

IRS Pub. 1075
NIST 800-53 Revision 4

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

Effective Date: 6/1/17

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to the DET Bureau of Security. As such, the DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version	Approval/Revision/Review Date	Description	Approver/Author, Title
.1	10/3/2016	Original Draft	Tanya Choice Cybersecurity Compliance Consultant
.2	10/12/16	Draft Approved by DET Audit and Compliance	J. Thompson, B. Farrar, T. Choice
1.	5/11/16	Final Draft	Bill Nash

Authorized and Approved by:

Bill Nash	Bill Nash	5/11/17
Print/Type	Signature	Date

Division of Enterprise Technology-Bureau of Security

Chief Information Security Officer

Effective Date: 6/1/17

Appendix A

The Classified, Restricted, Sensitive, and Public labels are determined by the impact level of high, moderate, low, or none as determined by the scores of three principles of security: 1) confidentiality, 2) integrity, and 3) availability.

Each of these three principles of security is individually scored (0 – 3) by impact level as public, low, moderate, or high, to indicate the impact to the enterprise if the threat was realized. For example, an information asset may have a confidentiality level of "3", an integrity level of "2", and an availability level of "1" (i.e., HML) for an overall score of 6 indicating a level of Sensitive. Information/criteria to define the impact level is provided in the Appendix A – Table: CIA Impact Criteria.

Appendix A Table: CIA Impact Criteria

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. 0 for Public Information	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. 1	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. 2	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. 3
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. 0 for Public Information	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. 1	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. 2	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. 3
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542] 0 for Public Information	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. 1	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. 2	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. 3

Source: Adapted from FIPPS-199

Classification Level

7-9	Classified
3-6	Restricted
1-2	Sensitive
0	Public